DISCOVERY COMPUTERS and FORENSICS

Digital Forensics • CyberSecurity Management

Law Firm CyberSecurity 2019 White Paper

> “According to Verizon’s 2018 Data Breach Investigation Report, 93% of data breaches are linked to email phishing and other social engineering.”

Introduction

Lawyers are in both the legal and the data management business. According to Verizon’s 2018 Data Breach Investigation Report, 93% of data breaches are linked to phishing and other social engineering incidents. These criminals successfully evade an organization’s security controls by using clever phishing and social engineering tactics that often rely on employee naivete. Emails, phone calls and other outreach methods are designed to persuade staff to take steps that provide criminals with access to company data and funds. Yet there’s an overlooked layer that can radically reduce an organization’s vulnerability: **security awareness training and frequent simulated social engineering testing**.

Client data comes in many forms, it is not just tax returns or lists of assets. In today’s digital world our personal and professional lives are filled with personal identifiable data and every lawyer and every member of their firms, regardless of size, have the ethical obligation to reasonably protect their clients’ information.

Take a moment to think about your personal and professional lives. Do you have banking apps on phones, order products using a credit card from your phone? In the professional environment, there are few areas that do not use a computer that captures sensitive data. Even if you “delete” the data, did you know that a shadow copy of that exists on the hard-drive? For these a and a long list of other reasons, a lawyer’s ability to protect client information has become more complicated and each lawyer or firm should enlist a subject matter expert to assist with developing a security policy and to monitor your devices for potential breaches.

Why would an untrained, inexperienced person attempt to resolve a complex issue such as cybersecurity on their own?

Afterall, you would think any person a fool if they represented themselves in court~ Right?

Many single practitioners say… ‘I am too small for a hacker to target.’ That is inaccurate, in fact smaller firms maybe a higher risk since hackers are listening to the single practitioner’s lack of cyber concern.

All law firms are attractive targets for hackers, because law firms often hold highly sensitive client data including confidential documents, tax returns, family investment accounts, trade secrets, proprietary business information and nonpublic financial information. This kind of data is a goldmine waiting to be exploited by hackers. It is not always about a cyber-criminal removing data to be exploited, hackers may attempt to lock the data and use ransomware or other schemes to extort sums of money from the breached law firm.

Email, file sharing, connecting onto unsecure Wi-Fi like a restaurant, coffee shop or even free municipality Wi-Fi give hackers potential routes of access, and the risk to the client and your reputation is clear.

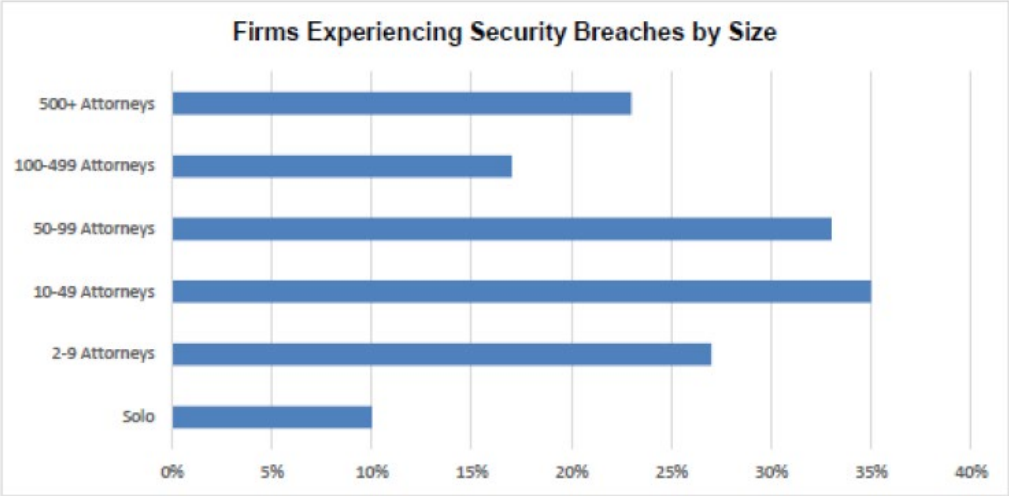
How many of you reading this recall the high profile cyberattack on the law firm in Panama that disclosed over 11 million confidential documents known as the Panama Papers? That was a big one, and the damage to the clients and the firm itself was immeasurable. The media is fast to report on huge breaches like the Panama Papers, but everyday small firms are attacked.

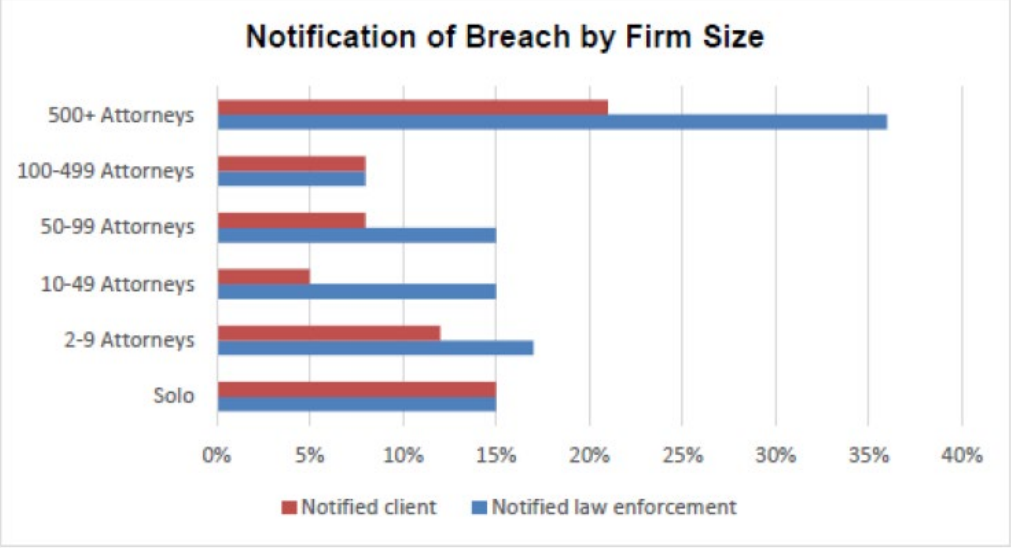
I read recently about Moses Afonso Ryan Ltd, a 10-lawyer firm in Providence, Rhode Island, which reportedly paid $25,000 in ransom following a ransomware attack that locked the firm's computer network (including the files on the network) for 3 months.

The firm subsequently filed a claim for lost billings of over $700,000. A claim that was denied by the insurer and they had to litigate. A black eye on top of a black eye! If this firm used a service like Discovery Computers and Forensics' Virtual Chief Information Security Officer or vCISO monitoring service that would have cost less than $1500 per month… the firm may have not lost over $725,000!

The ABA Cyber Security Handbook states: "law firms and lawyers… are increasingly required to know and understand data security and how it potentially affects their clients… Ignorance of the risk is no longer an option or excuse." All lawyers should work closely with a cybersecurity to develop a customized cybersecurity program that mitigates the eminent threat of data breach and meets the regulatory and compliance requirements of the firm and its clients. ABA Model Rules of Professional Conduct, Rule 1.6: Confidentiality of Information, section (c) states: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

According to the ABA Tech report approximately 27 percent of firms of 2-9 lawyers experience a data breach. 34 percent of law firms with 10-49 lawyers had some type of IT or data breach. Lawyers in the digital age are in both the legal and the data management business.





All firms, regardless of size need a good cybersecurity program that can remain dynamic and responsive to the ever-changing cyberthreat landscape and the growth of their law practice. The first step is to work with a trusted cybersecurity company to develop a security plan that is tailored to your needs. This plan should include computer monitoring for traditional I.T. support combined with security training. Even if you are a single practitioner with one assistant, you need a cyber plan and training to ensure you are compliant with ABA rules.

If your firm represents clients in heavily regulated clients in industries such as finance, healthcare and energy, for example, your cybersecurity vendor should ensure your security policies are following the policies of the firm's clients regarding SOX, HIPPA and others.

Most small or midsized law firms assign a staff lawyer to head the I.T. or cybersecurity. This is a great solution to meeting the compliance checklist. Utilizing a vCISO platform that leverages cyberthreat detection can lower costs instead of hiring a full-time employees.

Remember, people are the cause of most cyber-intrusions; this could include you! It is reported that over 80 percent of breaches are due to people unknowingly allowing hackers into the office. The most cost-effective method of security training can be executed by single lawyers as easily as firms with hundreds of attorneys. Law firms and their lawyers are bound by the American Bar Association Model Rules of Professional Conduct, so it is best practice that everyone understands their ethical and professional responsibilities.

Even the American Bar Association is a target. This week I read in an article from Law360 that the American Bar Association warned members to be wary of fraudulent email requests for dues payments, tweeting that scammers have been sending around bogus e-bills.

The example that the ABA posted asked members to pay their dues within 48 hours via a link to a "secure portal," or face revocation of membership.

Dear Attorney,

Your membership fees are 1 week overdue. Please log in to our secure portal to pay your fees.

Please do this within 48 hours or your membership will be revoked.

This is a courtesy reminder notice from the American Bar Association. If your account is no longer active, please update your account now so you no longer receive emails.

Sincerely,

Accounting & Finance
The American Bar Association

An email with an ABA letterhead and the following text: Dear Attorney, Your membership fees are 1 week overdue. Please log in to our secure portal to pay your fees. Please do this within 48 hours or your membership will be revoked. This is a courtesy reminder notice from the American Bar Association. If your account is no longer active, please update your account now so you no longer receive emails.

The State Bar of California sent out an alert in May warning attorneys licensed in the state to be aware of a phishing scam coming in the form of suspicious emails claiming that their fee payments to the bar are overdue.

A phony email purporting to be from the state bar included the subject line "Past due invoice for State Bar Association of California" and suggested that attorneys click on a link that will download an invoice, according to an alert posted on the state bar's website. The email told attorneys to pay the license renewal fee or face suspension, the bar's alert said.

So it is happening, there is no putting your head in the sand. Lawyers should take the necessary steps to protect client information and their reputation. The cost to do so is now a line item in the budget. If you are breached, having a cyber incident plan in place to isolate the threat and enact a preapproved communications plan is essential.

Do you have cybersecurity insurance? About 34 percent of law firms have cybersecurity insurance. This is a huge risk for uncovered firms when considering the average breach can cost as much as $4,000,000. Having a cybersecurity policy in place acts as the primary coverage policy should a breach occur and should not require the firm to turn to its professional liability coverage which may not adequately cover damages resulting from cyberbreaches.

In closing, regardless of the size of your law practice, contact a cybersecurity vendor to discover how to minimize the cybersecurity threats that do not cost a lot of money. It will cost something. Cybersecurity is an essential part of all businesses in the digital age, so set a budget and meet with an expert with the expertise that understands the legal industry and use them as required. Catalog your devices and determine the best method to keep them secure. Document policies train your employees with a minimum of annual onsite training and if you can afford it monthly web-based training that can cost as little as $39/month per staff member. Perform tests to determine points of weakness or employ a vCISO for less than a part-time bookkeeper would cost. Secure a cybersecurity insurance policy.

Taking these steps will put any lawyer or firm on the path to cybersecurity and ethics compliance.

About Discovery Computers and Forensics

A trusted partner since 2003, helping clients with their cybersecurity strategy and has performed hundreds of computer forensic examinations for a variety of legal and regulatory compliance matters.

Rod Mac Kenzie
Discovery Computers and Forensics LLC
p: 770.984.5000 m: 678.361.0036
a: 3690 N. Peachtree Rd. Ste 100-D
Atlanta, GA 30341
w: DiscoveryCF.com e: RodM@DiscoveryCF.com

DISCOVERY COMPUTERS and FORENSICS
Digital Forensics • CyberSecurity Management

Schedule a Free CyberSecurity Consultation